



Don't get hooked by phishing links

Microsoft Outlook Anti-Phishing Add-In

Team PhishTank

Sultan Baig, Ryan Ellison, Tameem Imamdad, & Stephanie Stiles

www.outphish.com

Abstract

Phishing emails are designed to steal passwords, banking and credit card information, and other sensitive personal information; tricking even technically-proficient email recipients into believing illegitimate messages originate from trustworthy sources. Team PhishTank has developed an Outlook add-in, called “OutPhish”, to help users detect phishing emails and avoid falling victim to attacks. OutPhish identifies known phishing links by leveraging the latest phishing threats and information through PhishTank and Google’s Safe Browsing services. Outphish quarantines suspect messages and disables their links, so users cannot accidentally browse to malicious pages. OutPhish also provides users the ability to proactively report suspicious emails, helping protect others in the OutPhish community against the newest attacks.

Table of Contents

Introduction	4
Phishing Overview	4
OutPhish Features	7
OutPhish Technical Information and Data Sources	9
Overview of OutPhish's Development Status	10
References.....	11
Appendix A.....	12
User Manual.....	12

Introduction

Phishing emails pose a legitimate threat to everyone. Companies have the concern of protecting their own and their customers' data. Consumers have a need to protect their own, personal information. Well-intended email users unknowingly participate in these scams by clicking on malicious links contained in phishing emails. They often end up providing sensitive data to malicious websites. These messages threaten the safety and security of company trade secrets, reputation and brand, sensitive and proprietary information, banking credentials, and many other forms of private data.

To counter the continual threat of new phishing attacks, a new Microsoft Outlook add-in, OutPhish, has been developed. OutPhish detects and quarantines suspected messages by identifying known dangerous links, and provides users the ability to proactively report other suspected suspicious links. With the use of OutPhish, users are provided additional protection against falling victim to even some of the most convincing phishing attempts.

Phishing Overview

Before examining the features of OutPhish and how it aims to protect its users, it is important to explain what phishing is. According to phishing.org, phishing refers to methods used to trick individuals or employees into divulging information or compromising computer system security, with attackers usually pretending to send communication on behalf of legitimate sources such as banks or online merchants. By tricking email recipients, they gather sensitive information such as login credentials, bank information, credit card numbers, and other confidential data ("What is Phishing?," n.d.).^[1]

Phishing attempts are classified into three categories: phishing, spear phishing, and whaling. General phishing attempts are just attempts that target the masses. They do not target anyone in particular. Spear phishing targets particular groups of people such as employees of a certain company or working within a specific department. Whaling aims attempts at high-level executives and people in notable positions.

Phishing emails are often visually indistinguishable from the legitimate messages they impersonate. According to Norton, related attacks such as sphere phishing can make messages even more convincing by carefully targeting messages to specific groups or individuals ("Sphere Phishing," n.d.).^[2] Without software tools to detect such attacks, everyday email users have little chance of being able to accurately differentiate between what is legitimate versus illegitimate. Meanwhile, advanced users may be able to detect a larger portion of phishing emails, but manual phishing-detection efforts take an undesirable amount of effort and time, and they are far from foolproof.

A phishing attempt example is outlined below. In Figure 1, a user receives an email, reported to be from, the Bank of America regarding some suspicious activity on their account. The source email address, the Bank of America logo, phone number, website address, subject of the message, and the body of the email all appear to look like a genuine Bank of America email notification. Without additional training, it is difficult to recognize that this message is fraudulent.

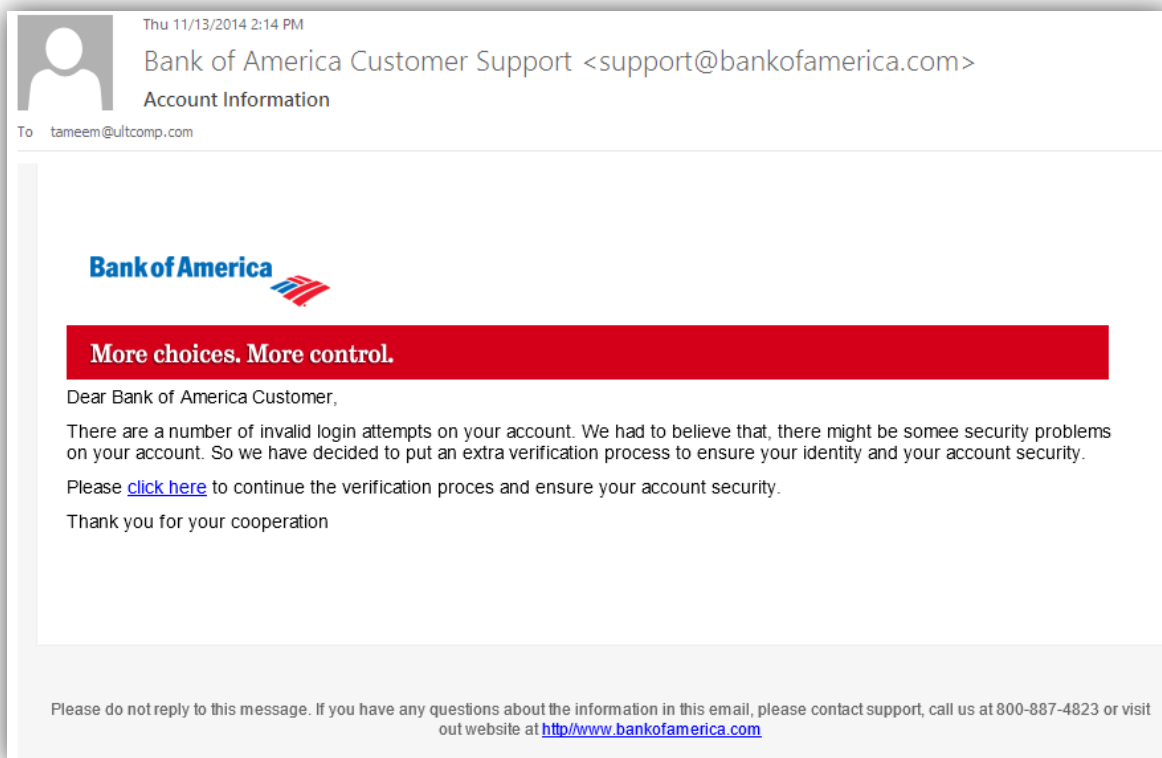


Figure 1: Email from Bank of America

However, analysis of Figure 2 demonstrates a source address of ultcomp@ultcomp.com and not the expected Bank of America web address.

```
0;">Dear Bank of America Customer,</p>&#13;
    <p style="font-family: 'Helvetica Neue', 'Helvetica', Helvetica, Arial,
padding: 0;">There are a number of invalid login attempts on your account. We had to believe tha
verification process to ensure your identity and your account security.&#13;
    <p style="font-family: 'Helvetica Neue', 'Helvetica', Helvetica, Arial,
padding: 0;">Please <a href="ftp://81.136.232.135/bankofamerica.htm">click here</a> to continue
    <p style="font-family: 'Helvetica Neue', 'Helvetica', Helvetica, Arial, sans-serif
0;">Thank you for your cooperation</p>
```

Figure 2: Email Header

Figure 3, illustrates that the “click here” text, in the body of the message, is linked to <ftp://81.136.232.135/bankofamerica.htm>, an FTP site and not the Bank of America site. This link is potentially a cloned Bank of America site. A user may click this link and believe that the website they are directed to is really the Bank of America. If the user attempts to login on the page by entering in their Bank of America login name and password, they may have just provided their credentials to a hacker who can now use that information to login to the user’s account. This gives the hacker full access to the user’s account and other sensitive private information. The hacker can now use the new information to gain access to other sites, records, and accounts, and the ability to setup new accounts. It is likely the first step in a long chain of events leading to identity theft. But, identity theft is not the only threat waiting on the web page. As the user attempts to login to the fake bank site, their PC may be downloading malicious programs and exploits. Trojans, malware, or key loggers installed in the PC can further compromise the user’s files and information. Key loggers log all of the keys that have been pressed on the keyboard, including login names and passwords. The captured data can automatically be sent to the hacker. The compromised PC can also become part of a botnet and used to carry out attacks to other sites or companies.

```
Return-path: <ultcomp@ultcomp.com>
Envelope-to: tameem@ultcomp.com
Delivery-date: Thu, 13 Nov 2014 12:13:52 -0800
Received: from ultcomp by ultcomp.com with local (Exim 4.82)
        (envelope-from <ultcomp@ultcomp.com>)
        id 1xp0m8-0008RI-5T
        for tameem@ultcomp.com; Thu, 13 Nov 2014 12:13:52 -0800
To: tameem@ultcomp.com
Subject: Account Information
Date: Thu, 13 Nov 2014 14:13:52 -0600
From: Bank of America Customer Support <support@bankofamerica.com>
Message-ID: <2abc825b17de5015eb211cd2ca8ff44a@ultcomp.com>
X-Priority: 3
X-Mailer: PHPMailer 5.2.7 (https://github.com/PHPMailer/PHPMailer/)
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 8bit
```

Figure 3: Source code of Bank of America Email – Click Here

```
color: #666; font-weight: normal; margin: 0 0 10px; padding: 0;">Please do not reply to this message. If you have any questions about the information in this email, please contact support, call us at 800-887-4823 or visit our website at <a href="http://login-apple.com/caf/Caisse-allocations-familiales">http://www.bankofamerica.com</a>
```

Figure 4: Source Code of Bank of America Email – Spoofed Web address

The figure above shows that The Bank of America web address is really a link to another site: <http://login-apple.com/caf/Caisse-allocations-familiales>. Figure 1 shows that the Bank of America website address is listed, along with other information, at the bottom of the phishing email. However, some analysis of the source code, reveals a spoofed web address. This demonstrates how preventative training and general knowledge about phishing is not enough. Without skilled understanding, people can easily fall victim to these tricky messages. OutPhish provides additional, necessary protection.

OutPhish Features

OutPhish was developed as an Outlook add-in, intended to be used by both individuals and businesses. OutPhish works by checking each link contained in incoming messages. The links are verified using Google's Safe Browsing API and PhishTank phishing services, and for enterprise users, OutPhish's own database of phishing data. Google's Safe Browsing service provides OutPhish with a continual stream of updated Google phishing data. PhishTank is a compiled list of phishing addresses reported by the on-line community. By using multiple services, OutPhish provides critical phishing protection and automatic functionality to its users.

When a phishing link is detected, the entire message is considered a threat. The user receives a prompt with guidance to quarantine the message or disable the links and keep it. The prompt also provides an option to view additional information about the suspicious link(s). OutPhish also offers an option to always remove the suspicious messages by default. In cases where a user finds a suspected phishing message has avoided detection, a feature allows the bad link(s) to be reported so that other users can be protected.

OutPhish's own database is especially valuable to defending organizations against spear phishing. Some links may not have been identified yet by the phishing listings. The OutPhish database is a way to retain the links that are not officially reported to the services. The database also offers flexibility and can be customized by an organization or business; allowing for increased protection and performance.

The OutPhish dashboard provides an efficient and user-friendly way for staff to monitor the organization for phishing attempts. It allows users and staff to view statistics, information on phishing threats, and configure personal or corporate options. OutPhish hosts the functionality and associated databases for personal users. Companies can host the database on local infrastructure if preferred. In addition, OutPhish offers to track of the reported Phishes. Users have the liberty to add bad links directly to the OutPhish website without waiting for an email to arrive containing the link.

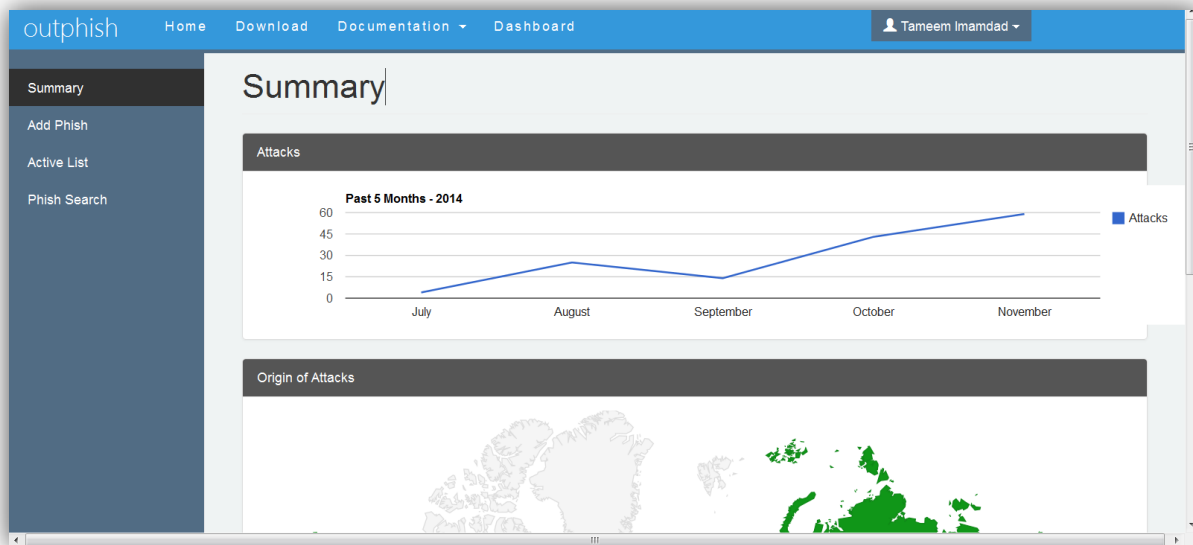


Figure 5: Origin of attacks and Statistics on www.outphish.com

OutPhish's reporting feature, "Report Phish," allows users to tag unidentified suspicious links. The feature was designed to counter zero-day attacks. Such attacks or new threats that have not yet been reported to PhishTank or Google Safe Browsing services. When users elect to report them, they are added to the OutPhish database and automatically reported to PhishTank. OutPhish continues to aid in a collaborative process by securing messages, even when attackers try to get ahead.

The following is an example of the pop-up window that an OutPhish user receives when an email that contains identified phishing links arrives in their inbox. The pop-up allows users to get more information about the phishing attempt and an option to delete the email or to mark it as safe and continue reading. If the user elects to mark it as safe, as a precaution, OutPhish disables the links in the message.

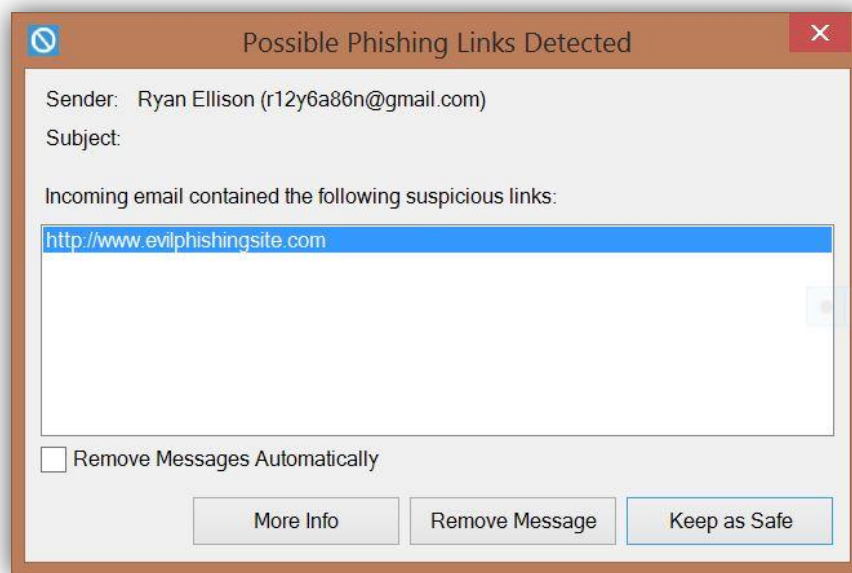


Figure 6: OutPhish Phishing Detection

OutPhish Technical Information and Data Sources

The OutPhish Outlook add-in was created using C# with Microsoft Visual Studio. The web dashboard was created with PHP. OutPhish's own databases make use of MySQL. The links contained in Outlook email messages are checked against Google's Safe Browsing API and PhishTank database.

PhishTank.com manages the PhishTank database. The PhishTank website is designed to be a free, collaborative, community-based site that allows users to submit and verify suspected phishing URLs, and FTP and IP addresses. It operates under the authority of well-known security company, OpenDNS. The information posted on the website is a shared community forum. PhishTank's database is continually updated as users submit bad links. PhishTank ensures not to reveal any information that may harm or expose the reported data or targeted users ("What is PhishTank?," n.d.).^[3]

Google designed, and operates, the Google Safe Browsing Service. According to the Developers Guide at developers.google.com, its main function is to provide a continually updated list of malicious URLs containing phishing data or malware. OutPhish sends each link to Google for verification of status. Google replies to OutPhish with a result that the link is malicious or not ("Developers Guide," n.d.).^[4] Unlike PhishTank, Google Safe Browsing service does not collect any data from users. Instead, it uses tally count to analyze how many people visited a forged site.

Overview of OutPhish's Development Status

The creation and development of OutPhish has followed the Software Development Life Cycle steps and processes. Team PhishTank continues to refine and improve the user experience and functionality of OutPhish to provide the best security possible.

References

^[1]*What is Phishing?. (n.d.). Phishing.org. Retrieved October 22, 2014, from <http://www.phishing.org/what-is-phishing/>*

^[2]*Spear Phishing: What It Is and How to Avoid It | Norton. (n.d). Retrieved November 3, 2014, from <http://us.norton.com/spear-phishing-scam-not-sport/article>*

^[3]*PhishTank | Join the fight against phishing. (n.d). Retrieved November 3, 2014, from <https://www.phishtank.com/faq.php>*

^[4]*Developer's Guide (v3). (2014, June 26). Retrieved November 4, 2014, from https://developers.google.com/safe-browsing/developers_guide_v3*

Appendix A

User Manual

outphish

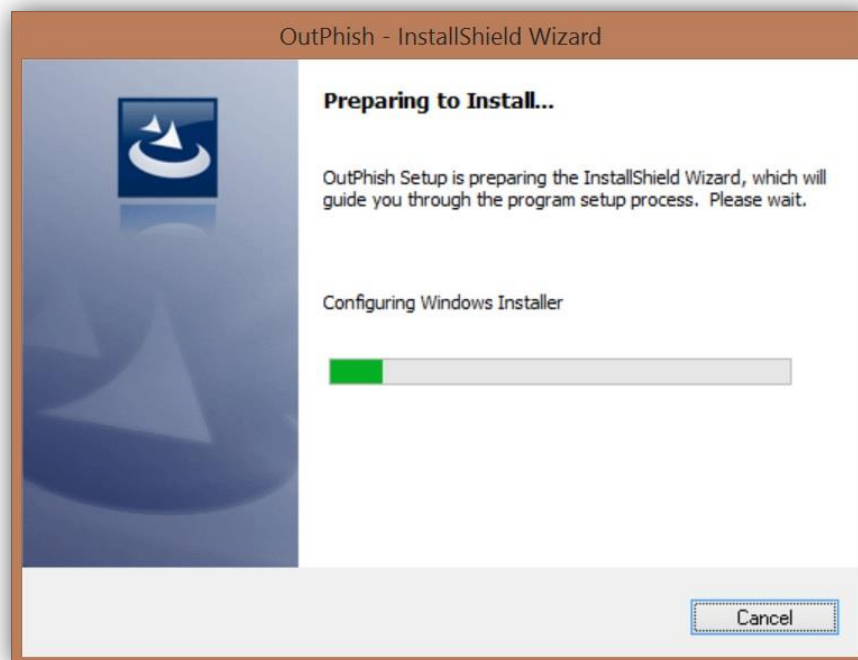
Don't get hooked by phishing links

Installation and User Guide

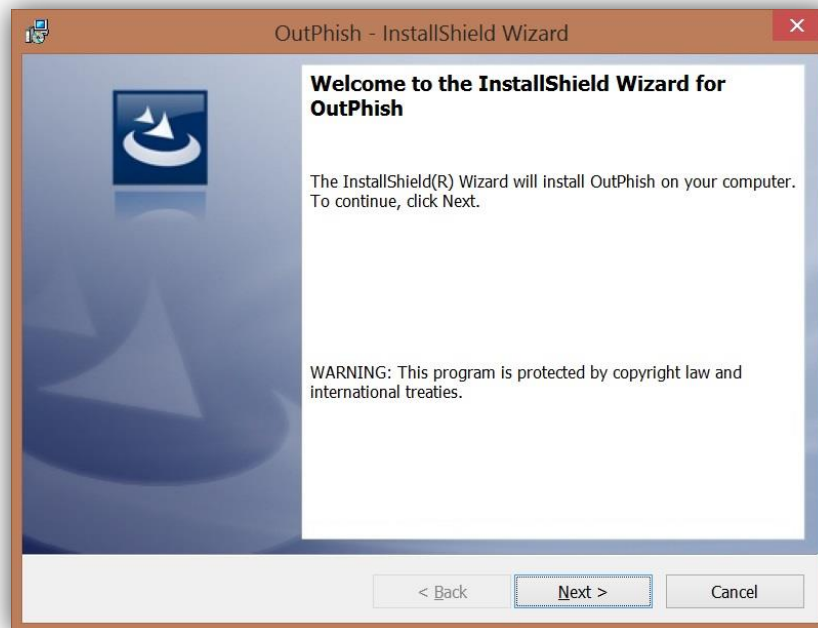
OutPhish is an outlook add-In that checks incoming email messages for phishing links. If the suspicious links are found in the body of the message, they will be flagged and automatically disabled. OutPhish uses its own database and leverages PhishTank and Google Safe Browsing services for harmful link identification. If the user suspects a message contains links that were not identified as malicious, but is potentially harmful, an option is provided to allow users to report the link(s).

OutPhish Installation

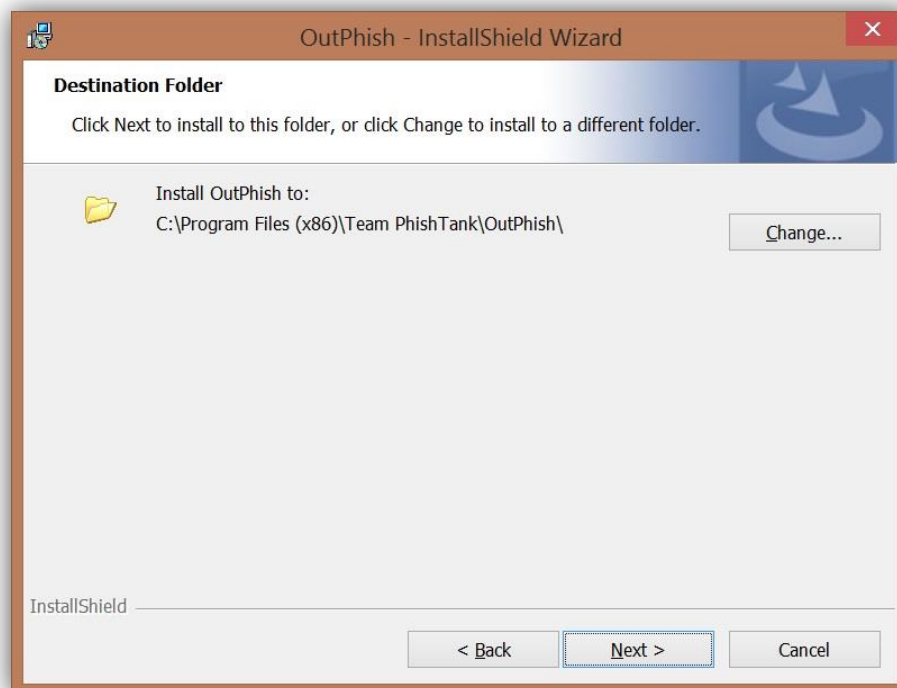
1. Launch the OutPhish install file. The OutPhish - Install Shield Wizard window will appear and the installation begins.



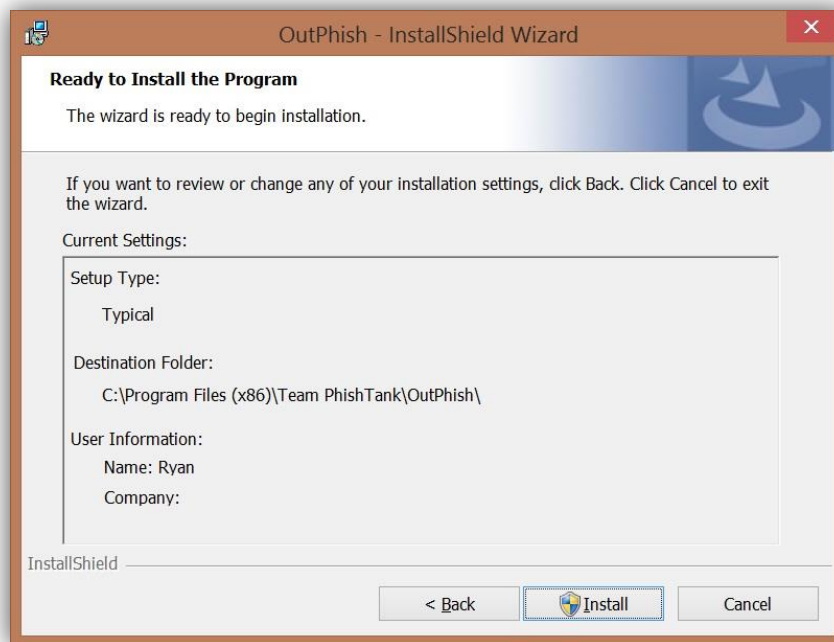
2. A Welcome message is displayed and the user is prompted.
Click **Next** to continue the installation.



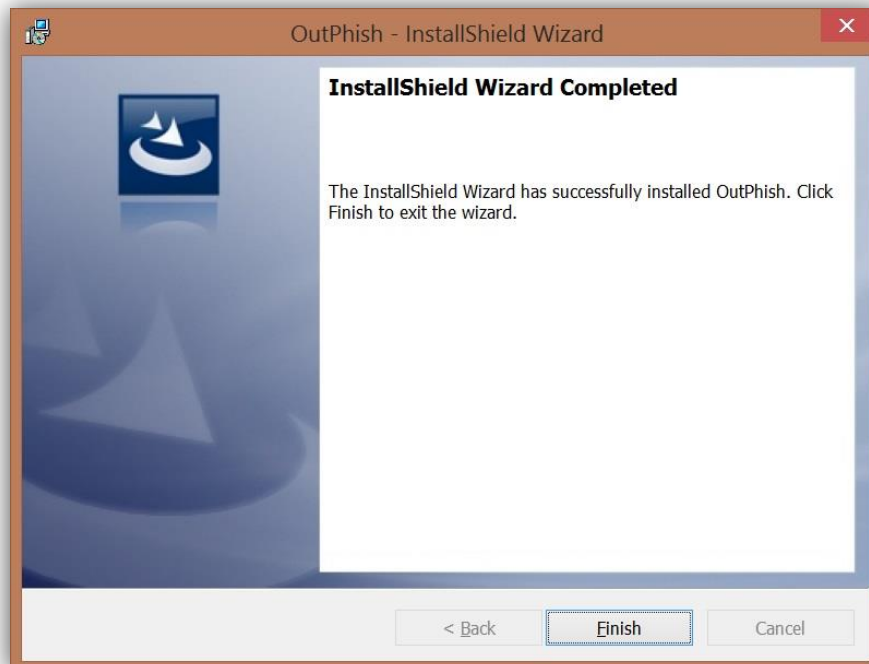
3. To accept the default program destination folder, click **Next**.
To select a different folder path, click **Change...**
Parse to the desired path and click **OK**.
Click **Next** to continue.



4. To continue the installation with the settings shown in the Current Settings box, click **Install**. Click **Back** to go back to any of the previous steps and update the settings, then continue as prompted.



5. Upon notification that the installation is complete, click **Finish**.



Using Øutphish

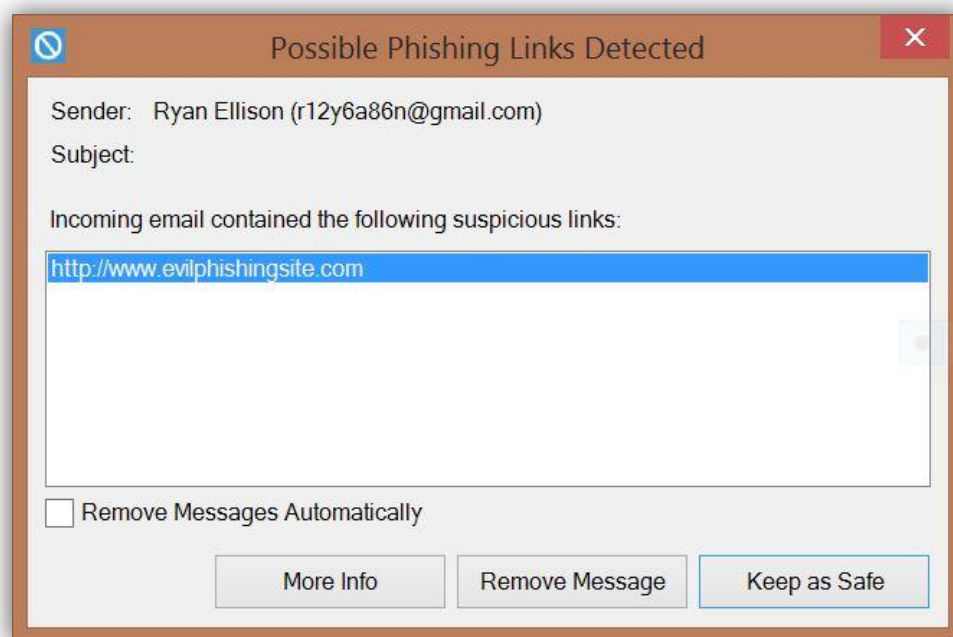
Tagged Links

Open Outlook or navigate to your Inbox.

Øutphish automatically scans all incoming email and checks all links contained in the messages.

Øutphish first checks URLs, and FTP and IP addresses against the Øutphish database for reported links. If links in the message are bad, the user will receive a pop-up message notifying them that the message contains bad links. If bad links are not found, Øutphish then checks with PhishTank and Google Safe Browsing services for known bad links.

When at least one bad link has been identified by the local database, Phishtank, or Google Safe Browsing, the pop-up message below appears. Any link found in the message that is bad will be displayed in the Possible Phishing Links Detected box.



There are 3 options for selection:

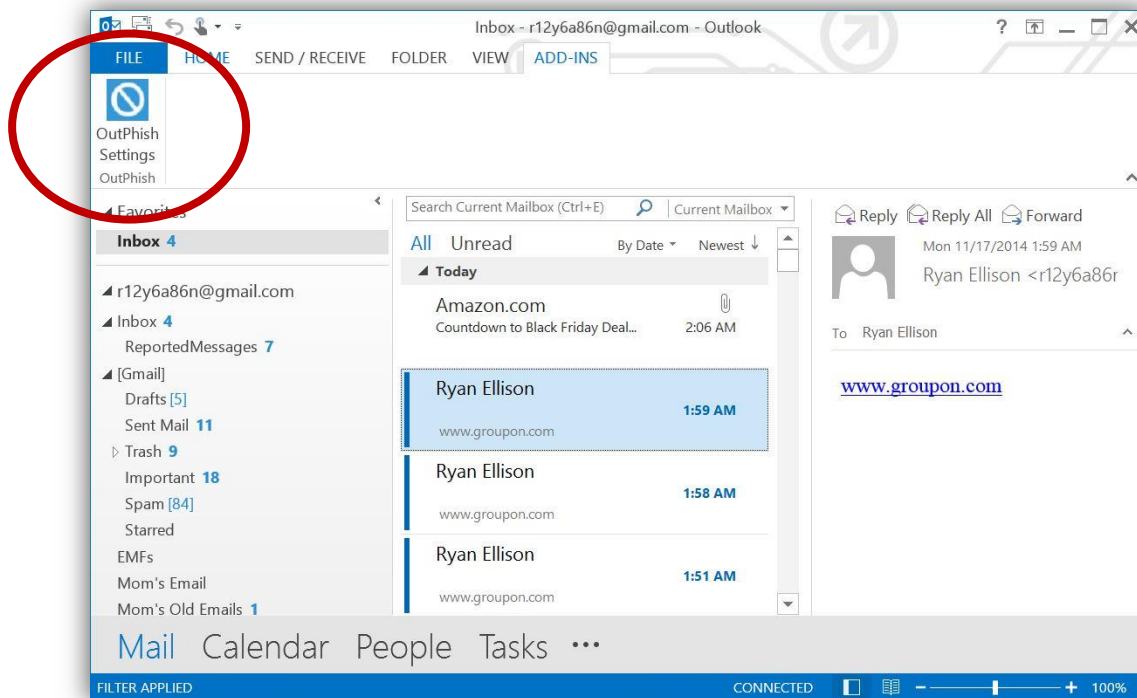
More Info will open a browser page containing information about the link.

Remove Message will move the suspicious message(s) to the Reported Messages folder.

Keep as Safe will retain the message in the Inbox; however, the links in the message will be disabled.

To automatically remove known phishing emails, and no longer be prompted for action selection, click to check the box, near the bottom right, to **Remove Messages Automatically**.

To view OutPhish settings, click the button from the toolbar.



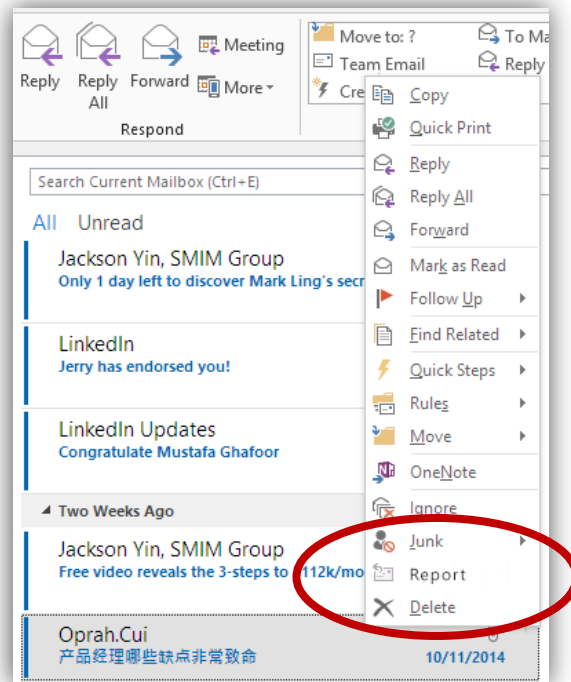
After clicking the Settings button, the user is prompted to enter their OutPhish login credentials.

A screenshot of the "OutPhish Settings" dialog box. The title bar says "OutPhish Settings". The main area is titled "OutPhish Home". It contains three input fields: "OutPhish Database:" with the value "outphish.com", "Username:" with the value "Ryan", and "Password:" with the value "*****". Below these fields is a checkbox labeled "Remove Phishing Emails Automatically" which is checked. At the bottom right are two buttons: "Save Settings" and "Cancel".

The user will be directed to the OutPhish control panel. See accompanying information regarding the control panel below.

Reporting Links

To report a suspected malicious link, highlight the message containing the link, and right-click. Select **Report** from the menu.

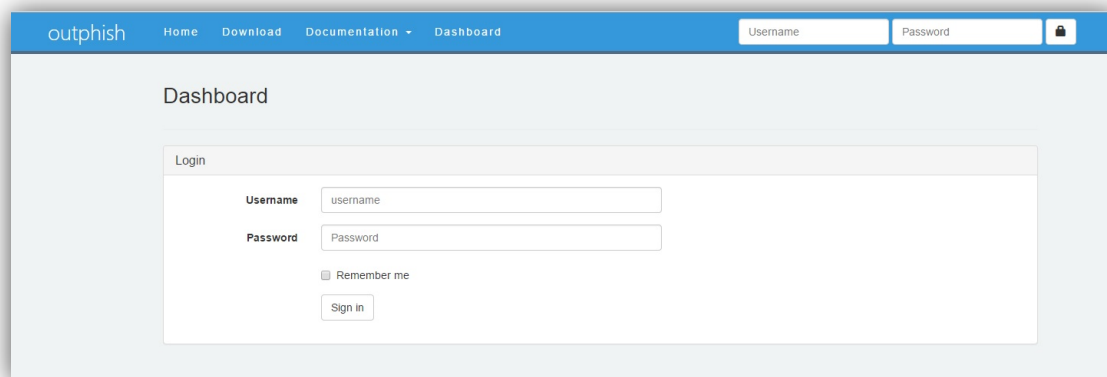


The link will be automatically reported on the user's behalf.

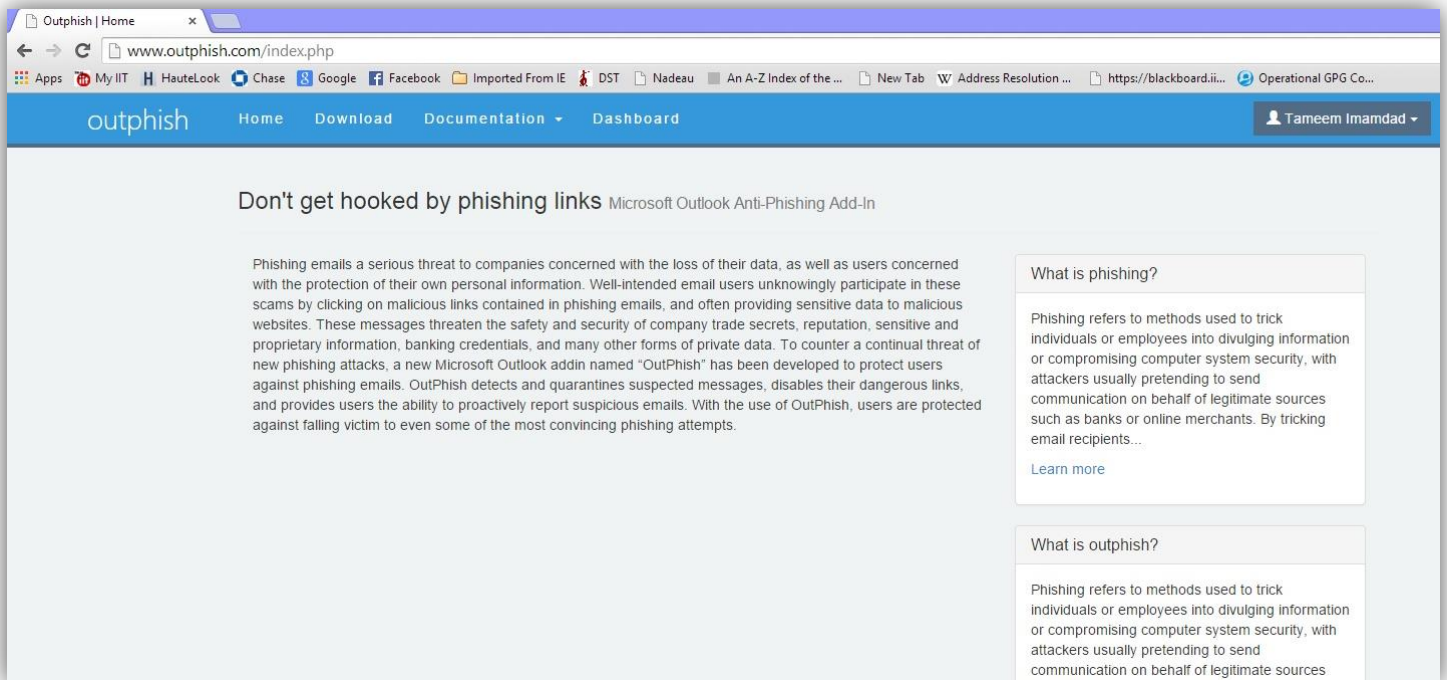
Øutphish Control Panel

Øutphish provides a control panel including a web dashboard. The control panel provides one convenient location to change settings, find documentation, and view statistical information.

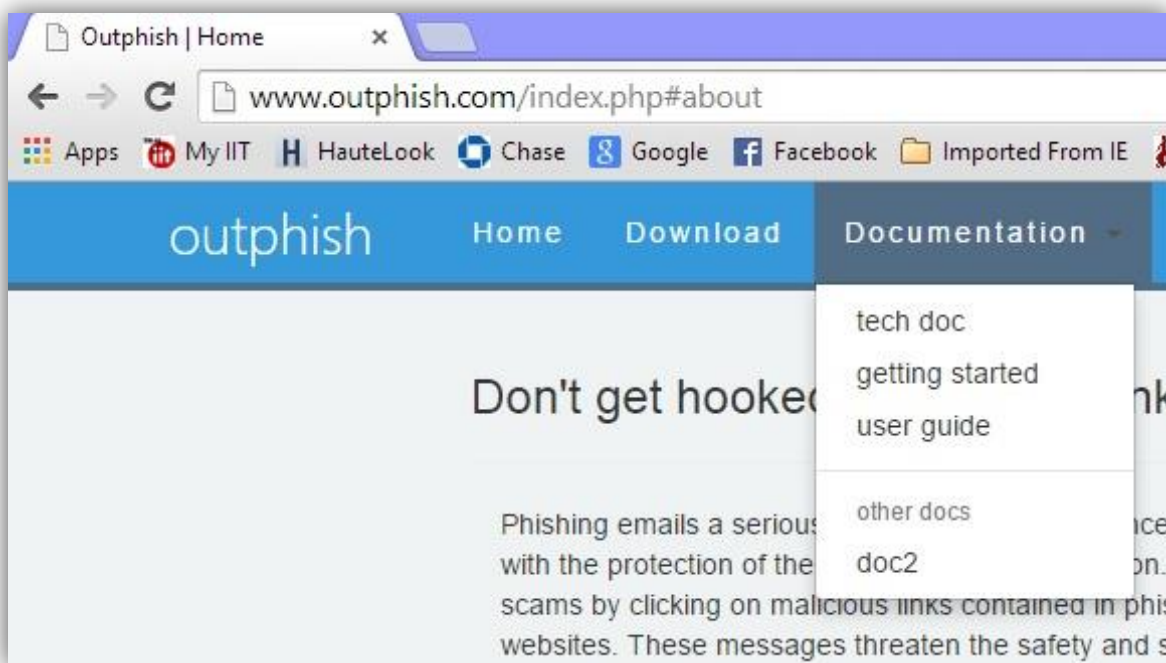
Navigate to outphish.com. Enter the assigned **Username** and **Password**. Click **Sign In**.



At the **Home** page, the user can click to learn more about phishing or Outphish.

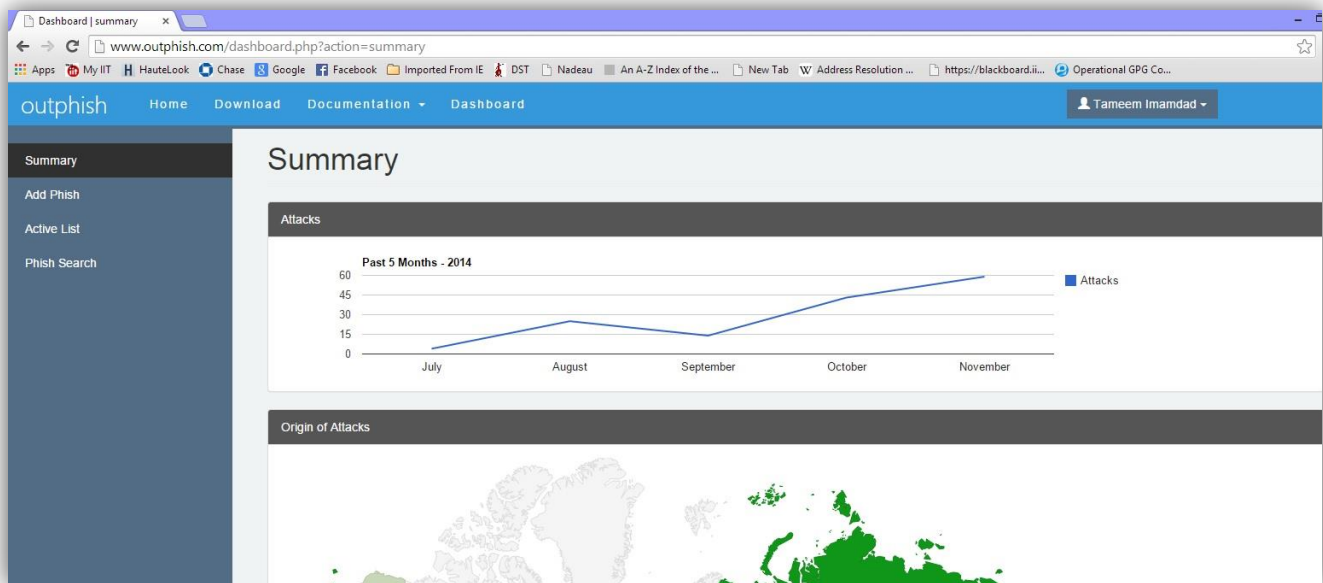


To view relevant documentation, select Documentation then highlight the desired document.



Select **Dashboard** from the toolbar to view statistics, add bad links, and view the bad links list.

Select the **Summary** tab from the left menu bar to observe gathered stats from phishing attempts.



Select the **Add Phish** tab to add bad links to the Phishing List that may not be known.

Type in the **URL** at the prompt.

Enter in any associated information in the **Description** box.

The screenshot shows the 'Add Phish' form. It has two input fields: 'URL' with the placeholder text 'url' and 'Description' with the placeholder text 'insert description'. Below the fields is a blue 'Add' button.

Select the **Active Phish** tab to view the URLs that have been added to the list.

Click the trash can icon to the left to remove any link that is no longer needed on this list.

The screenshot shows the 'Active Phish List' table. It has three columns: ID, URL, and Description. There are three rows of data. Each row has a trash can icon to its right.

ID	URL	Description
1	google.com	sample insert
2	sample.com	test
3	gssskjfdjfs.com	